PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/32

A2

(11) International Publication Number: WO 98/45982

(43) International Publication Date: 15 October 1998 (15.10.98)

(21) International Application Number: PCT/NO98/00109

(22) International Filing Date: 2 April 1998 (02.04.98)

(30) Priority Data:
971605 8 April 1997 (08.04.97) NO

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON [SE/SE]; S-126 25 Stockholm (SE).

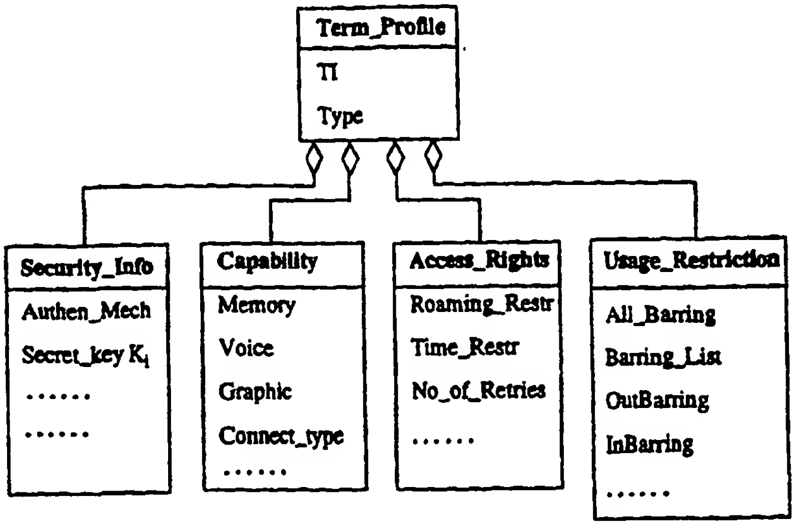
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: THANH, Do, Van [NO/NO]; Stjernemyrveien 28, N-0673 Oslo (NO).

(74) Agent: OSLO PATENTKONTOR AS; Postboks 7007 M, N-0306 Oslo (NO).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: ARRANGEMENT FOR IMPROVING SECURITY IN A COMMUNICATION SYSTEM SUPPORTING USER MOBILITY



The Information object Term_Profile

(57) Abstract

The present invention relates to an arrangement for improving security in a communications system, especially a telecommunications system, said system comprising distributed hardware and software components which interact in order to provide services to one or more users, and for the object of implementing this improvement this can according to the present invention be done by introducing in said system a generic access control. In a specific embodiment the invention suggests three types of access control especially related to access to the terminal in question, to the telecom system and to the requested services.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

ARRANGEMENT FOR IMPROVING SECURITY IN A COMMUNICATION SYSTEM SUPPORTING USER MOBILITY

FIELD OF THE INVENTION

The present invention relates to an arrangement for improving security in a communications system, especially a telecommunications system, said system comprising distributed hardware and software components which interact in order to provide services to one or more users.

More specifically the present invention concerns a user access control for distributed systems that support user mobility, i.e. users are allowed to move and use different terminals to access services.

BACKGROUND OF THE INVENTION

The Access control is the procedure used by the telecom system domain to ensure that the user accesses the telecom system domain in accordance with the restrictions specified at subscription [1]. When mobility is supported, every user will have the possibility to use any terminals at any access points. The access control procedure is also intended to limit the access capability of a user for the protection and privacy of third party. The third party can be the owner of the terminal or the access point, and must have the right to block or deblock, suspend or reset the service delivery at his terminal or access point to a user.

When the user is allowed to move and access to the telecommunication services anywhere and at any time, the risk of threats increases dramatically at the same time as the mechanisms necessary to enforce security become more difficult to realise. In systems supporting general mobility, fraudulent use of anyone's subscription can be attempted from any terminal and at any network access point. In this way the user may be exposed to various forms of fraud as, for example, fraudulent use of the user `s resources by unauthorised parties who manage to take up the identity of the user, eavesdropping, unauthorised tapping or modification of information exchanged during communication, and disclosure of the user's physical location [4]. Another security problem arises because the user is allowed to use any terminal and at any network access point. Such a temporary usage may conflict with the use of the terminal by the terminal owners, also referred to as third parties [6]. In principle, third parties should not suffer in terms of loss of privacy or freedom of actions as a result of activities by the mobile user.

STATE OF THE ART

With mobility, users may make use of any existing and available terminals and network access points. However, this does not mean that the terminal owner (the third party) has to accept such actions on his terminal. He must have the rights to restrict the usage of the terminal, e.g. only allowing certain users while others are prohibited from using the terminal.

This may be done in many ways, e.g. by keeping the terminal in a secured place, use local password, etc., but such measures are cumbersome for the owner and often not secure enough. This is commonly referred as the protection of third parties.

The UPT (Universal Personal Telecommunication) [4] system comprises some sort of access control mechanisms but they are limited to telephony services and to voice terminals or telephone.

Consequently, there is a need for an improved user access control for distributed systems supporting user mobility.

OBJECTS OF THE INVENTION

The present invention has for an objective to address any mobile distributed system, any types of applications, i.e. voice, data, image, video, interactive, multimedia, etc., for in such mobile distributed systems to introduce an improved access control.

A further object of the present invention is to introduce a generic access control in such distributed systems.

Still another object of the present invention is to introduce such a generic access control for distributed systems supporting user mobility which can be used in mobile distributed systems comprising public or private, local-area or wide-area, wireline or wireless networks.

BRIEF DISCLOSURE OF THE INVENTION

The above objects are achieved in an arrangement as stated in the preamble, which primarily is characterised by introducing in said system a user access control, for thereby enforcing security in communications systems.

In other words, the invention also suggests that this type of generic access control is related to personal mobility.

Further features and advantages of the present invention will appear from the following description taken in conjunction with the enclosed drawings, as well as from the appending patent claims.

BRIEF DISCLOSURE OF THE DRAWINGS

Fig. 1 is a schematic diagram illustrating the main subject matter to which the present invention is related, namely by illustrating a user's access to the services in question.

Fig. 2 is a schematic diagram illustrating an embodiment of the present invention for carrying out access control, especially in relation to a information object Term_Profile.

Fig. 3 is a schematic diagram illustrating an embodiment of a Terminal_Data object.

Fig. 4 illustrates a computational model of the access control of a user for use of a terminal.

Fig. 5 is a schematic diagram illustrating a user_registration object containing a list of allowed services.

Fig. 6 is a schematic diagram illustrating the relation between user domain, terminal domain and telecom system domain as well as an embodiment of access control on the access to the telecom system.

Fig. 7 is a block diagram illustrating the relation between user domain, terminal domain and telecom system domain, as well as an embodiment of access control on the axis to the telecom system.

DETAILED DESCRIPTION OF EMBODIMENT

As stated previously, the present invention relates to user access control for distributed systems that support user mobility which means that the users are allowed to move and use different terminals to access services available to them.

In Fig. 1 there is illustrated a user which has access to a terminal which in turn is communicating with a telecom system which in turn is offering a plurality of services.

Before allowing the user to access the services offered by the telecom system domain, he is subject to three types of access control

- access control concerning the use of the current terminal (protection of third party)

- access control concerning the access to the telecom system

- access control concerning the use of the service requested

SOLUTION

We shall successively describe the three mentioned access controls.

Access control for use of the current terminal

With mobility, users may make use of any existing and available terminals and network access points. However, this does not mean that the terminal owner (the third party) has to accept such actions on his terminal. He must have the rights to restrict the usage of the terminal, e.g. only allowing certain users while other are prohibited from using the terminal. Of course, there are many ways to do this locally, e.g. keep the terminal in a secure place, use local password, etc. but they are cumbersome for the owner and often not secure enough. This is commonly referred as the protection of third parties [2].

Let us suppose that the mobile distributed system uses agent techniques to support mobility and has the following objects:

PD_UA (ProviderDomain_UserAgent) representing a user in the telecom system domain.

TA (TerminalAgent) representing a terminal in the telecom system do main

SPA (ServiceProvider Agent) representing the telecom system in the terminal domain

NAP representing a Network Access Point

TAP representing a Terminal Access Point

The information required for to carrying out the access control is contained in the Usage_Restriction component of the object Term_Profile (see Figure 2) which contains information about the terminal. The attribute All_Barring is used to specify that only the terminal owner can use the terminal. The terminal owner may also prevent a particular user or group of users from using his terminal by specifying the attribute Barring_List or to allow only certain user by specifying an Allowance_List. Modification of the Usage_restriction may be provided as an application where only the owner has the right to make access. The details of such an application and the specific layout of the Usage_Restriction is a matter of implementation and will not be carried further here.

In order to support selective access control of the terminal, the object Terminal_Data which contains information required for the support terminal mobility such as state, NAPid, etc. may be equipped with a table of controlled and cleared users, called ClearedUserTable, as shown in Figure 3. The ClearedUserTable contains the references or CIIs (Computational Interface Identifier) of the PD_UAs whose access have been controlled.

The TA assumes the Access control Enforcement Function (AEF). The Access control Decision Function is allocated to an object called ADF. The access control Procedure for use of the terminal is shown in Figure 4.

1. Every time an operation OpX arrives at the TA, the TA will check whether the identifier of the originating or addressed PD_UA is on the ClearedUserTable or not. If it is, TA will do the transfer of OpX If it is not, TA will initiate the access control Procedure.

2. TA invokes Get(Usage_Restriction) on Term_Profile to acquire the access control Decision Information (ADI).

3. The TA invokes the operation Decision_Request on the ADF object. The arguments of this operation are the ADI obtained from the

Term_Profile. The ADF makes the decision and returns the Access_Result to TA. The Access_result may be granted or not_granted.If the Access_Result is not_granted, TA returns an error message to the originator of the operation.

4. If the Access_Result is granted, TA invokes the operation Update(CleareduserTable,PD_UARef) on Terminal_Data to register the PD_UA of the newly cleared user.

One way of removing entries from ClearedUserTable, i.e the identifier (reference) of a PD_UA, is to restart a timer each time that entry is accessed. If the timer times out, the entry is removed. Some entries may be permanent, i.e. they are not associated with a timer.

This type of access control is only intended to other users than the terminal owner himself. In fact, the terminal owner should never be prevented to use his terminal. The access to the telecom system domain and the access to the services are different types of access controls which are applicable to all the users including the terminal owner.

In the object Usage_Restriction it is therefore necessary to define an additional attribute called NoRestr_List containing the PD_UA identifiers of the users who are by default allowed to use the terminal. The identifier of the terminal owner's PD_UA is one of them. This list must not be accessible to anyone but the telecom system domain operator itself, i.e. even not to the terminal owner. However, it may be possible to define an "emergency user", i.e. every call to an emergency number will be effectual without being checked by the access control service.

Access control for access to the telecom system domain

If the user is allowed to use the terminal, it does not necessarily mean that he is allowed to access the telecom system domain. He may be located outside the roaming area; his credit with the operator may have run out; the authentication mechanism used to authenticate him may also be too weak and he is allowed to access a limited set of services. The list of allowed services for a user at a terminal is hence equal to or smaller than the list of subscribed services. This list is a column in the User_Registration object in Figure 5.

The initiator of the access control service is User$_a$. The target is the telecom system domain. The AEF is assumed by the PD_UA$_a$. The ADF is assumed by the object ADF. The access of the user to the telecom system domain may be limited by some parameters such as Roaming_Restriction, Credit_Limit, Time_Restriction, etc. which are contained in the Service_Restriction attribute of the User_Profile object. The Service_Restriction attribute contains also a list of subscribed services. The use of the services in this list may be conditioned by the strength of the method used to authenticate the user, the location of the terminal, the call destination, etc. The Service_Restriction attribute may thus be quite complex.

A computational model of the access control service for access to the telecom system domain is shown in Figure 6.
The access control procedure is as follows:

1. The PD_UAa object invokes a Get(Service_Restriction) on the User_Profile to acquire the access control Decision Information (ADI).

2. The PD_UAa object invokes a Get(SecurityData) on the User_Registration object to acquire the contextual information (result from the authentication service).

3. The PD_UA$_a$ object invokes the operation Decision_Request on the ADF object. The arguments of this operation are the ADI obtained from User_Profile and the contextual information obtained from User_Registration.

The ADF may use the access control services offered by the platform or a security system to obtain further contextual information such as time, system status, etc. and the access control policy rules. The ADF makes the decision and returns the Access_Result to PD_UAa together with SecurityData and AllowedServices.

The Access_result may be granted, not_granted or suspended. If the Access_Result is Suspended, depending on the access control Policy the terminal will be, temporarily or permanently no longer allowed to access the telecom system domain.

If the Access_Result is not_granted, the SecurityData returned to the PD_UA$_a$ from the ADF will contain a NoOfRetries field increased by one. The NoOfRetries field indicates the number of unsuccessful access attempts and is used as contextual information for the next access control service. The PD_UA$_a$ will invoke the operation Set(SecurityData) on the User_Registration object to save the updated SecurityData. Depending on the operation which initiated the access control procedure, the PD_UA$_a$ will return the appropriate response containing a not_granted status.

When the Access_Result is granted, the AllowedServices containing an updated list of allowed services is returned to the PD_UA$_a$. The PD_UAa will invoke the operation Set(AllowedServices) on the User_Registration object to save the updated AllowedServices. Depending on the operation which initiated the access control procedure, the PD_UA$_a$ will return the appropriate response containing a granted status.

The user can now request the wanted service and is hence subject to the access control for the requested service.

Access control for the requested service

There are two types of services, outgoing and incoming. Outgoing services are initiated by the user himself while incoming services are delivered to him by other users or applications.

For outgoing services, the initiator of the access control service is Usera. For incoming services the initiator is some other user or application. The target is the requested service. The AEF is assumed by the PD_UA$_a$. The ADF is assumed by the object ADF. The access of the user to the requested service is limited by the information contained in the Allowed-Service list of the User_Registration object. Another restriction originates from the Usage_Restriction contained in the object Terminal_Data and set by the terminal owner. The terminal owner may allow only one or both of the two service types to be performed on his terminal The attributes OutBarring and InBarring of the Usage_Restriction is used to specify, respectively, the users who are not allowed to use outgoing services and incoming services on the terminal (or who are allowed).

The access control procedure is as follows:

1. The PD_UA_a object receives a ServiceReq(ServId) from either the user or an application.

3. The PD_UAaobject invokes a Get(Usage_Restriction) on the TA.

3. The PD_UA_a object invokes a Get(AllowedService) on the User_Registration.

2. The PD_UA_a object invokes the operation Decision_Request on the ADF object. The arguments of this operation are the ADI obtained from the User_Registration object and the TA.

The ADF makes the decision and returns the Access_Result to PD_UA_a. The Access_result may be granted or not_granted. Depending on the operation which initiated the access control procedure, the PD_UA_a will return the appropriate response to the requester. The access control on the requested service is shown in Figure 7.

MERITS OF THE INVENTION

This invention has high level of flexibility in the sense that it can be used in different mobile distributed systems, public or private, local-area or wide-area, wireline or wireless.

It is a complete access control in the sense that it contains all the three types of access control.

Important features of the invention may be listed as follows:

1: A user access control is introduced for distributed systems that supports personal mobility.

2: Such a user access control consists of access control for the use of the terminal, access control to the telecom system and access control to the requested services.

REFERENCES

1. ISO/IEC. Information technology - Open System INterconnection - security frameworks in Open Systems: Part 1: Access Control, Jun 93

2. ETSI. NA:UPT: Service Requirements on protection of third parties. Version 1.0.0

3. ITU-TS Draft recommendation F.851. Universal Personal Telecommunication (UPT) - Service Description. International Telecommunication Union-Telecommunication Standardization Sector, (Version 10) Jan 94.

4. ETSI. NA:UPT: Service Requirements on protection of thirdparties. Version 1.0.

Patent claims

1. Arrangement for improving security in a communications system, especially a telecommunications system, said system comprising distributed hardware and software components which interact in order to provide services to one or more users,
characterized by introducing in said a generic access control therein for thereby enforcing security.

2. Arrangement as claimed in claim 1,
characterized in that said generic access control is related to personal mobility.

3. Arrangement as claimed in claim 1 or 2,
characterized in that said generic access control is introduced in any Open Distributed Processing (ODP) system and/or any common Request Broker Architecture (CORBA) system, or similar.

4. Arrangement as claimed in any of the preceding claims,
characterized in that said generic access control is introduced in any mobile distribution system, offering any type of applications, i.e. voice, data, image, video, interactive, multimedia, etc.

5. Arrangement as claimed in any of the preceding claims,
characterized in that before any user is allowed to access the services offered by the related telecom system domain, the user will be subjected to several types of access controls.

6. Arrangement as claimed in claim 5,

characterized in that said access control preferably comprise access control for the use of the terminal, access control to the telecom system and access control to the requested services.

7. Arrangement as claimed in any of the preceding claims, characterized in that the information required for carrying out said generic access control is contained in a Usage Restriction component of a Term Profile object containing information about the terminal in question.

8. Arrangement as claimed in claim 7, characterized by a Terminal Data object containing information required or supporting terminal mobility, for example state, NAPid (Network Access Point id), etc., said object also comprising a table of controlled and cleared users.

9. Arrangement as claimed in claim 7 or 8, characterized in that said Term Profile object and said Terminal Data object which are found in the telecom system domain, are controlled by agent techniques, comprising inter alia a Terminal Agent (TA).

10. Arrangement as claimed in any of claims 7-10, characterized in that in the telecom system domain there is provided one or more timers which are restarted each time and entry is accessed the setting of the timer deciding the maintenance of said entry, and that entries not associated with a timer is regarded as permanent entries.

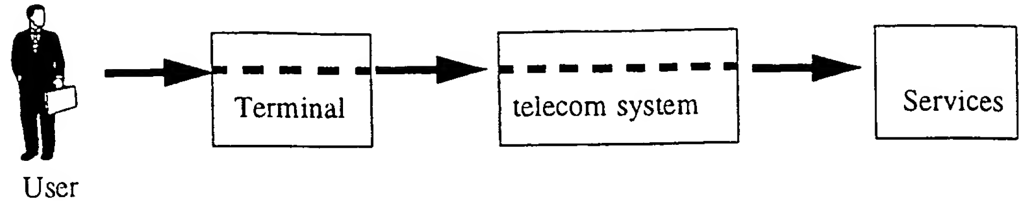


Figure 1 The user's access to the services

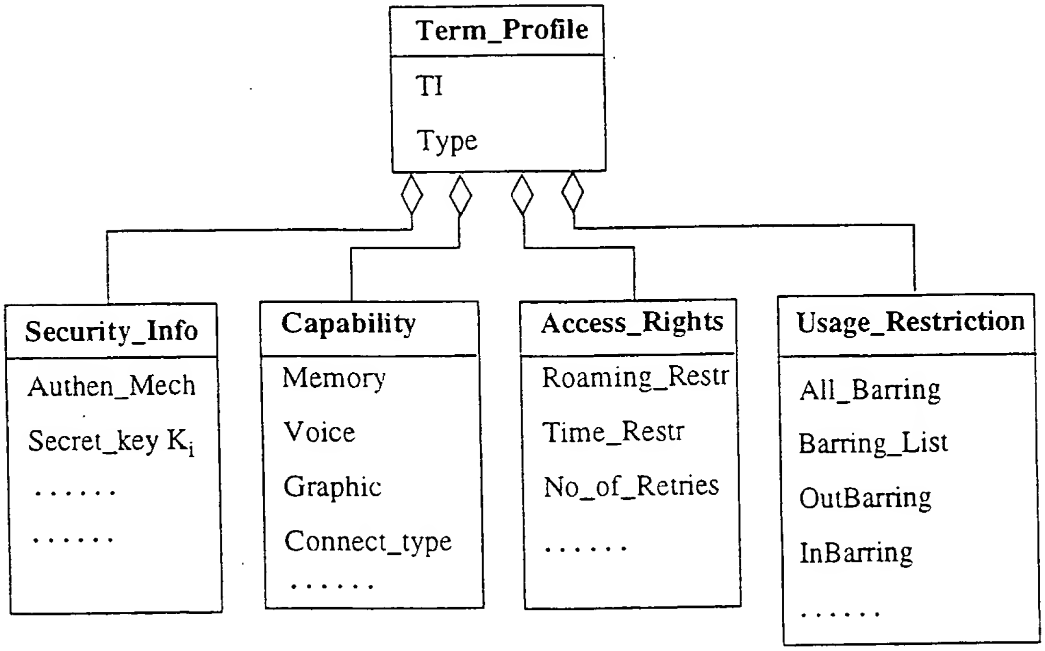


Figure 2 The Information object Term_Profile

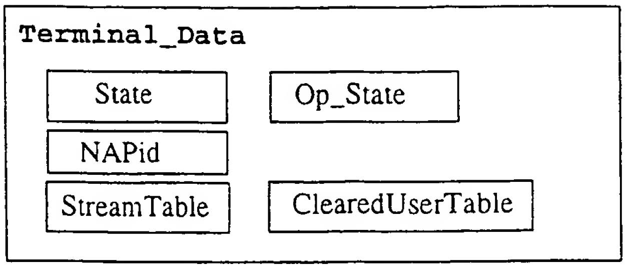


Figure 3 The Terminal_Data object

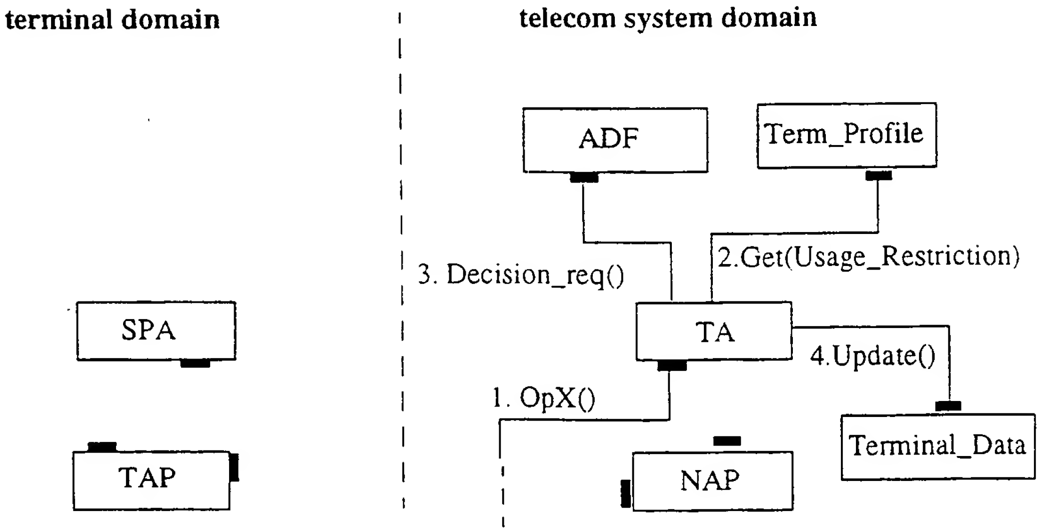


Figure 4 A computational model of the access control of the user for use of the terminal

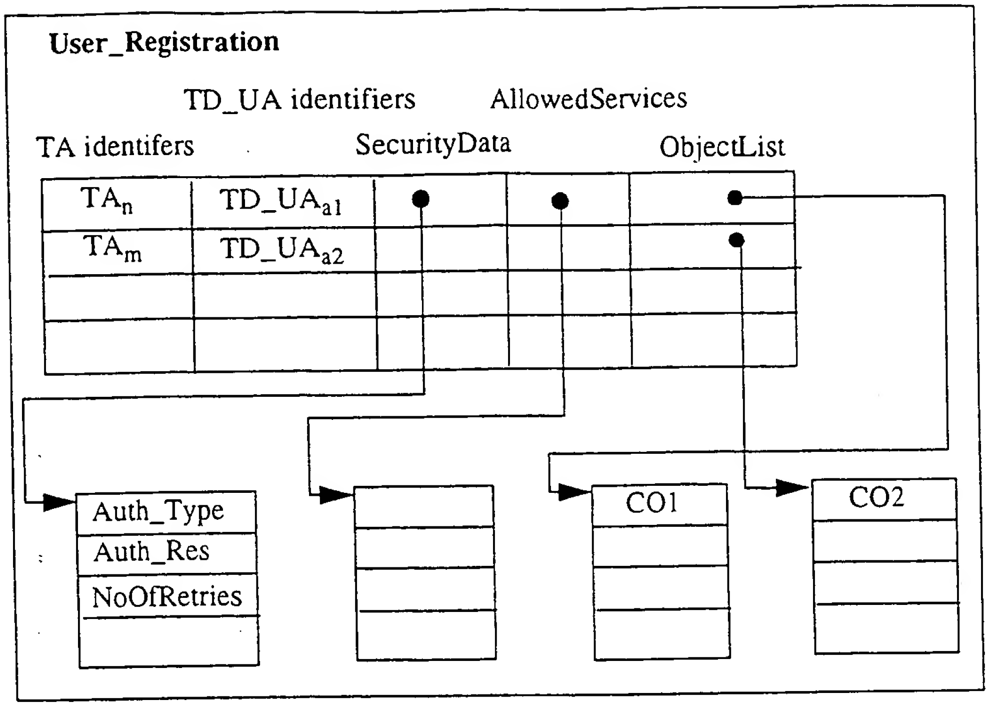


Figure 5 A User_registration object containing the list of allowed services

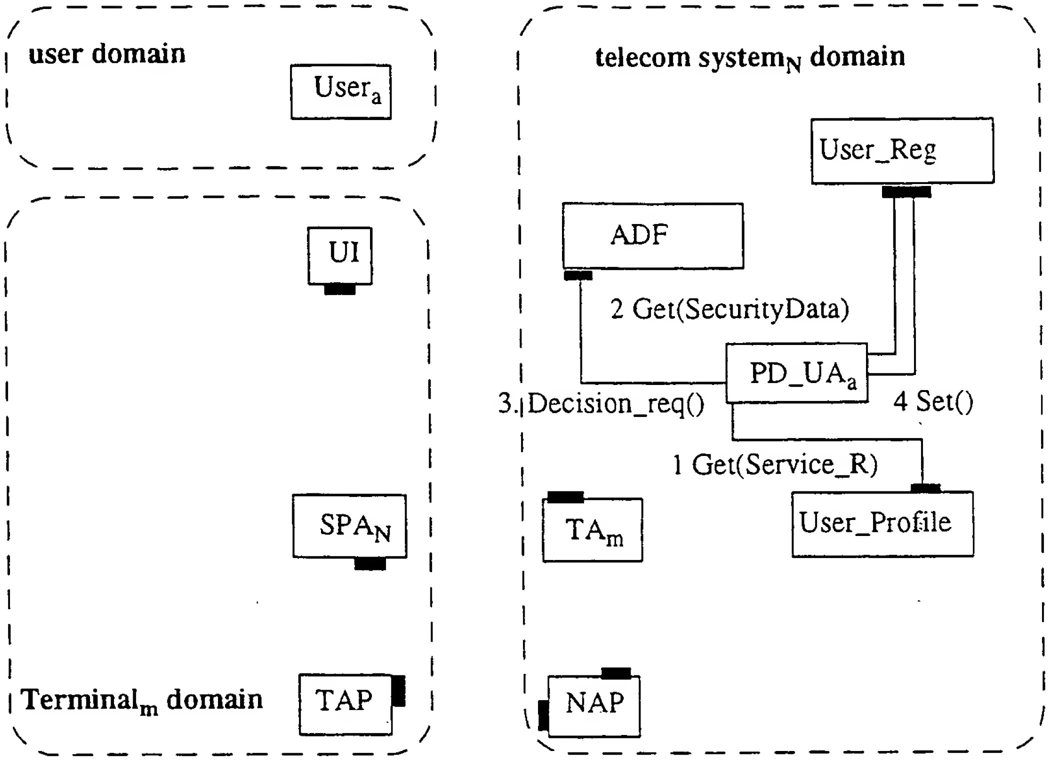


Figure 6 access control on the access to the telecom system

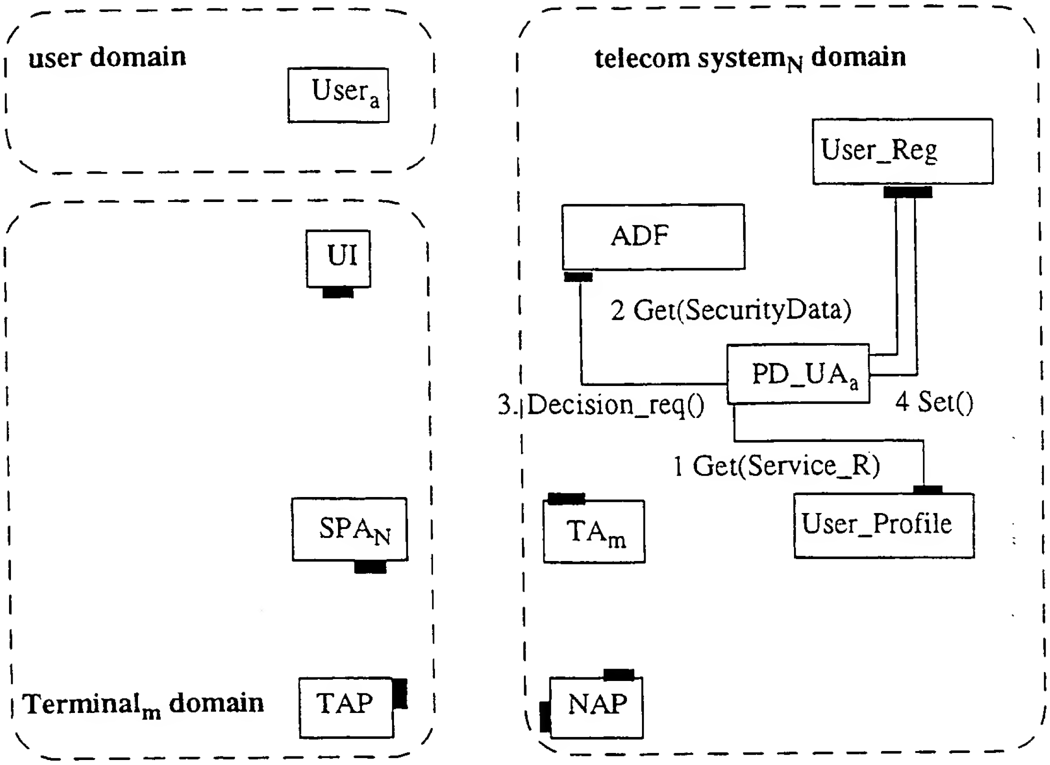


Figure 7 access control on the access to the telecom system

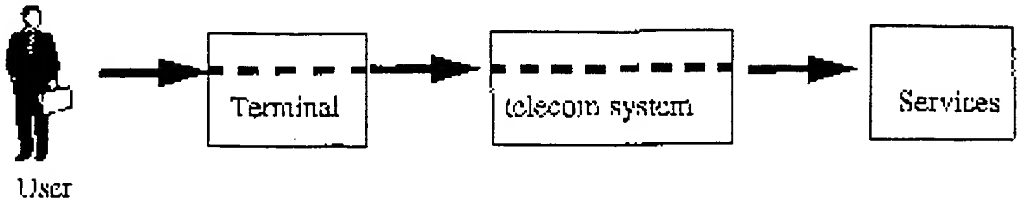


Figure 1 The user's access to the services

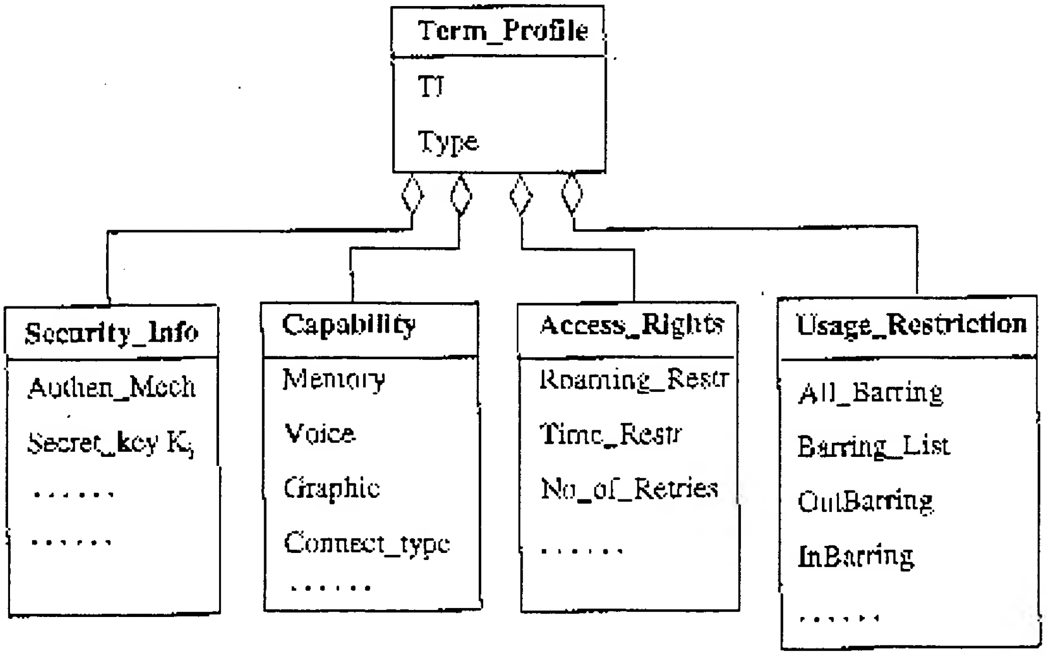


Figure 2 The Information object Term_Profile

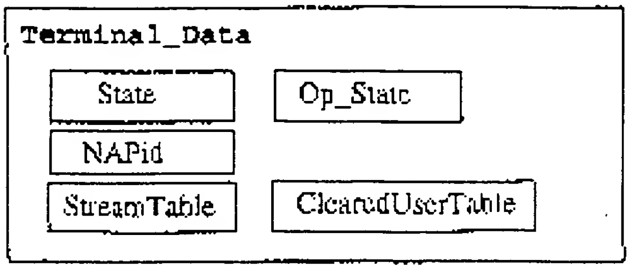


Figure 3 The Terminal_Data object

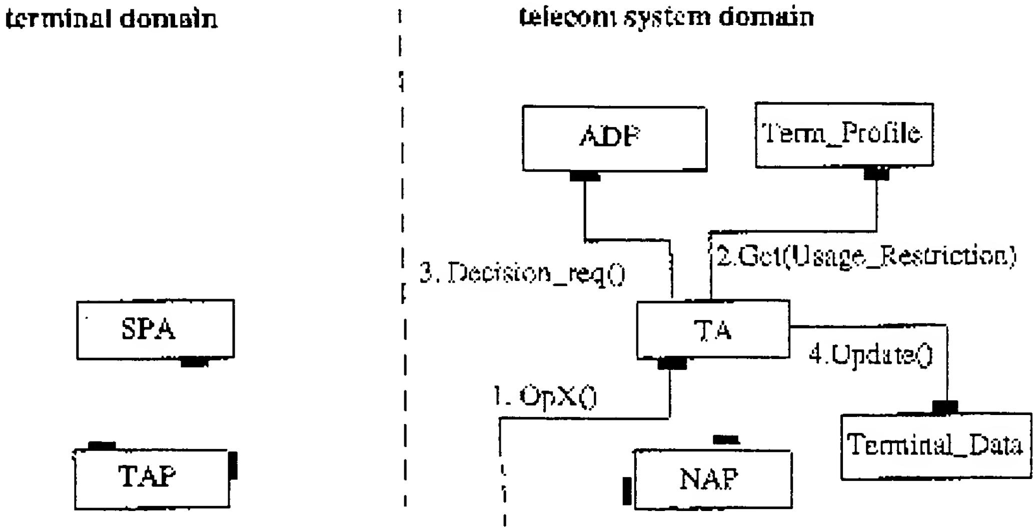


Figure 4 A computational model of the access control of the user for use of the terminal

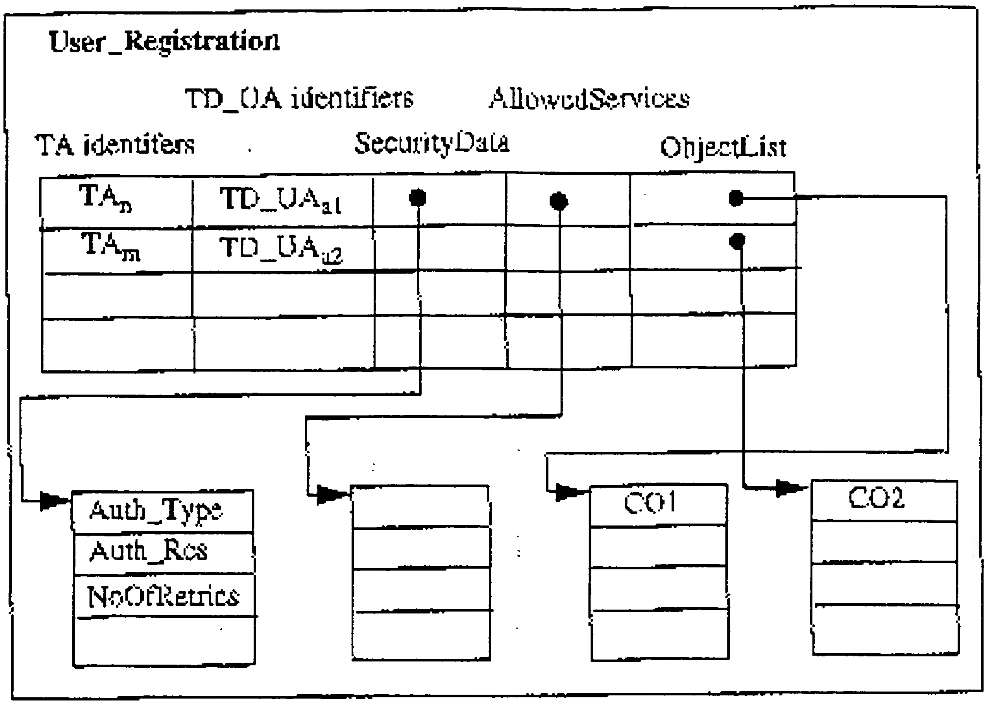


Figure 5 A User_registration object containing the list of allowed services

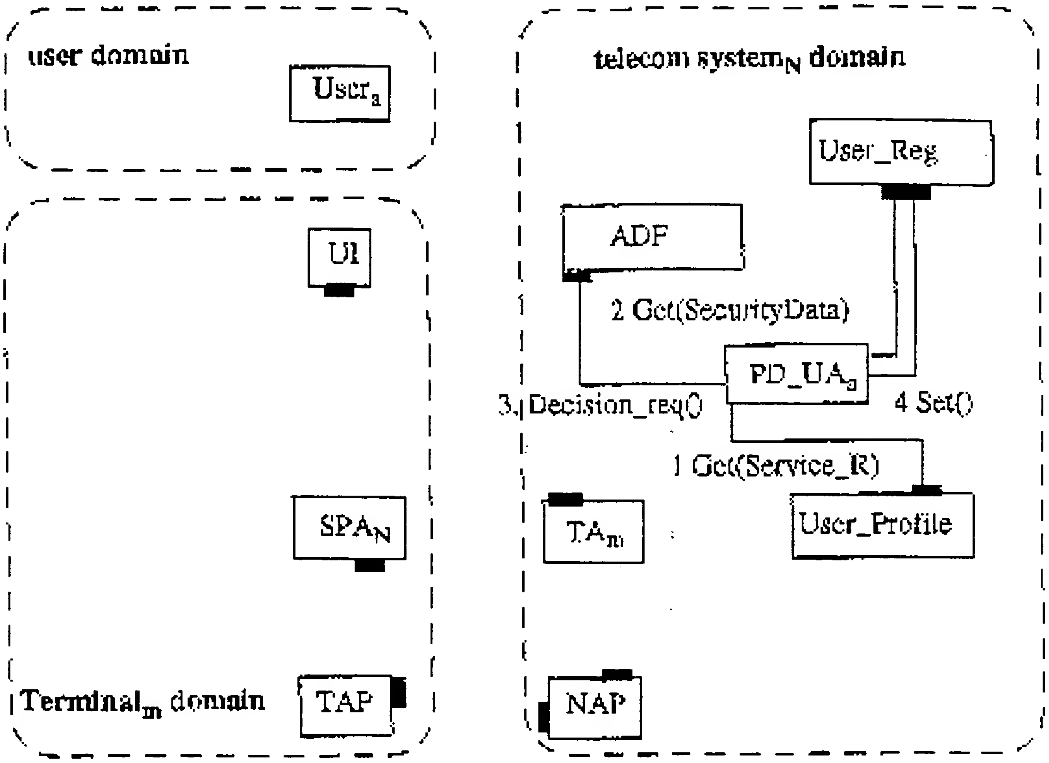


Figure 6 access control on the access to the telecom system

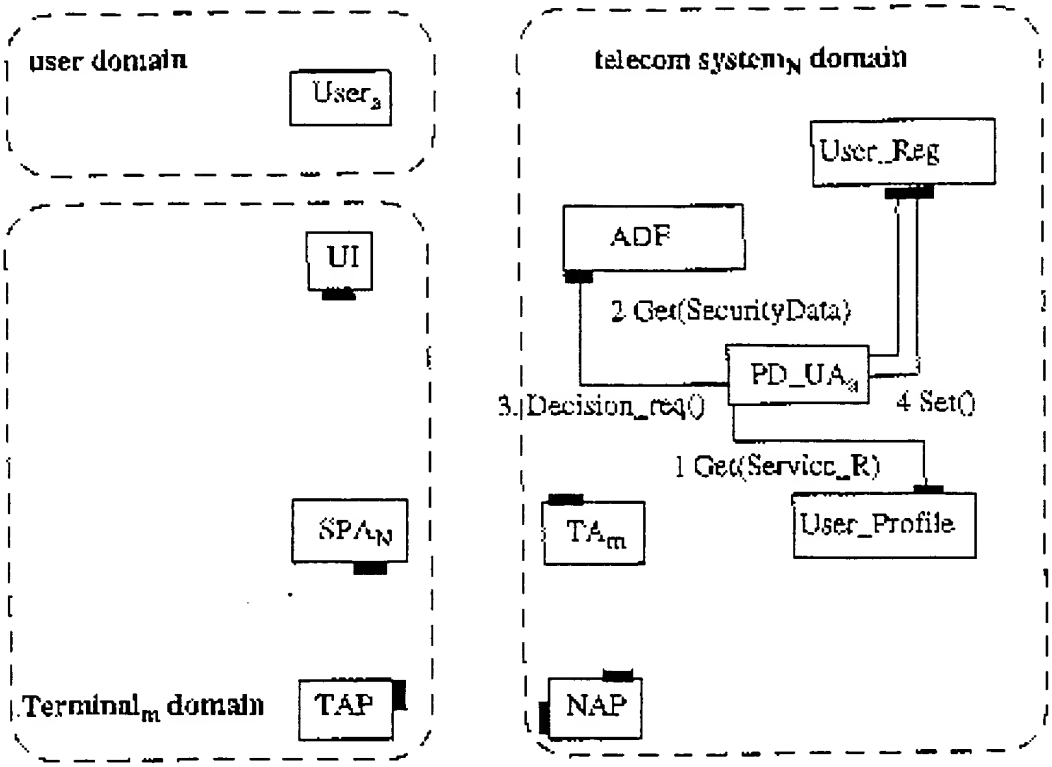


Figure 7 access control on the access to the telecom system

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04Q 3/00, G06F 9/46, H04L 9/32**	A3	(11) International Publication Number: **WO 98/45982** (43) International Publication Date: 15 October 1998 (15.10.98)

(21) International Application Number: PCT/NO98/00109

(22) International Filing Date: 2 April 1998 (02.04.98)

(30) Priority Data:
971605 8 April 1997 (08.04.97) NO

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON [SE/SE]; S–126 25 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: THANH, Do, Van [NO/NO]; Stjernemyrveien 28, N–0673 Oslo (NO).

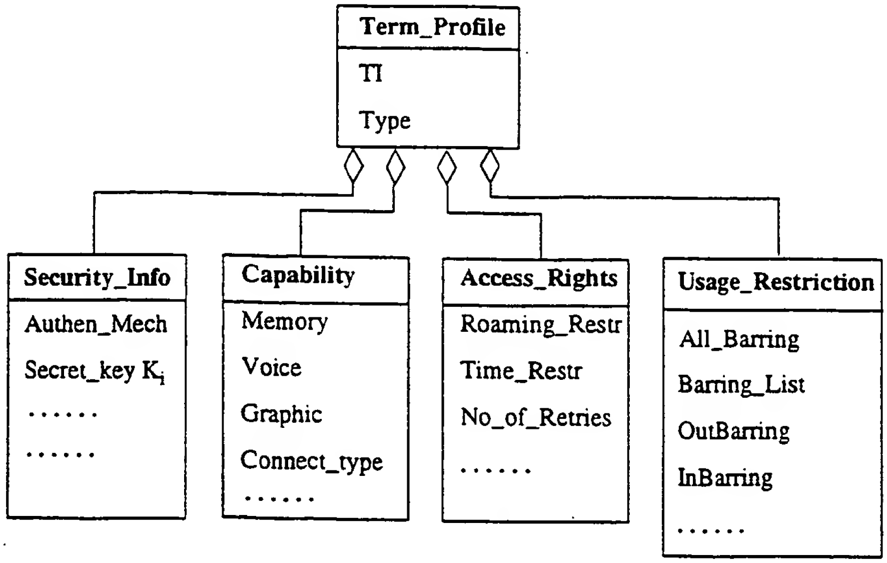
(74) Agent: OSLO PATENTKONTOR AS; Postboks 7007 M, N–0306 Oslo (NO).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report: 10 December 1998 (10.12.98)

(54) Title: ARRANGEMENT FOR IMPROVING SECURITY IN A COMMUNICATION SYSTEM SUPPORTING USER MOBILITY



The Information object Term_Profile

(57) Abstract

The present invention relates to an arrangement for improving security in a communications system, especially a telecommunications system, said system comprising distributed hardware and software components which interact in order to provide services to one or more users, and for the object of implementing this improvement this can according to the present invention be done by introducing in said system a generic access control. In a specific embodiment the invention suggests three types of access control especially related to access to the terminal in question, to the telecom system and to the requested services.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 98/00109

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 3/00, G06F 9/46, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04Q, H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

INSPEC, WPIL, EDOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	IEEE 46th Vehicular Technology Conference, Volume, 1996, (Atlanta, Georgia, USA), van Thanh et al, "Making Mobility Transparent to the Applications" page 1825 - page 1829 --	1-10
P,A	IEEE Communications Magazine, Volume, March 1998, Juna Pavón et al, "CORBA for Network and Service MAnagement in the TINA Framework" page 72 - page 79 --	1-10
A	IEEE Computer SocietyPress, Volume, November 1995, (Tokyo, Japan), Choong Seon Hong et al, "Service and Connection Management Architecture for distributed multimedia applications" page 296 - page 304 --	1-10

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 12 October 1998	Date of mailing of the international search report 15 -10- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Patrik Rydman Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 98/00109

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Telektronikk, Volume, 1994, Tom Handegård, "The TINA Consortium" page 74 - page 80 --	1-10
A	WO 9625012 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY), 15 August 1996 (15.08.96), page 1 - page 15 -- --------	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/07/98

International application No.

PCT/NO 98/00109

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9625012 A1	15/08/96	AU 4629196 A	27/08/96
		CA 2212377 A	15/08/96
		EP 0808545 A	26/11/97
		FI 973240 A	03/10/97
		GB 9508283 D	00/00/00
		NO 973623 A	06/10/97

This Page Blank (uspto)